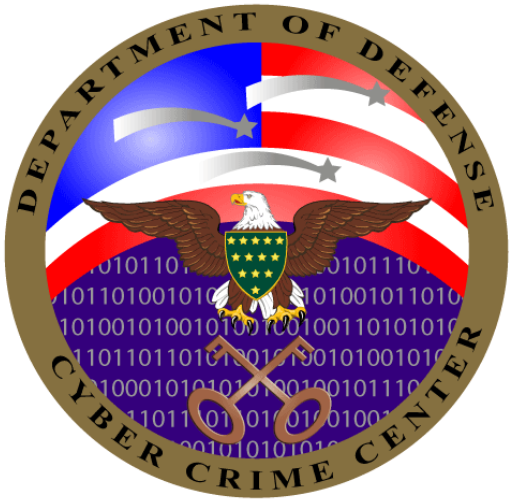

2010 DC3 DIGITAL FORENSICS CHALLENGE RULES
v1.2

16 February 2010

Rules Change Summary

Section	Change Description	Date Changed
2.2.4	Personal Information update clarification	17 Dec 09
8.0	Clarification on team disqualification rules	17 Dec 09
6.0	Intellectual Property Section rewrite	17 Dec 09
10.0	Addition of Privacy Policy section	17 Dec 09
5.2.2	Addition of SANS prize for Graduate students	01 Feb 09
5.3.1	Update of Post Graduate to Graduate language	01 Feb 09
2.2	Clarification of determination of team affiliation	16 Feb 09
2.2	Clarification of updating team member information	16 Feb 09
8.0	Update to team disqualification rules for falsification of information	16 Feb 09

Table of Contents

1.0 INTRODUCTION

1.1 Background

The Department of Defense Cyber Crime Center (DC3) sets standards for digital evidence processing, analysis, and diagnostics for any DOD investigation that requires computer forensic support to detect, enhance, or recover digital media, including audio and video. DC3 assists in criminal, counterintelligence, counterterrorism, and fraud investigations of the Defense Criminal Investigative Organizations (DCIOs) and DOD counterintelligence activities. It also supports safety investigations, the Inspector General, and commander-directed inquiries. DC3 aids in meeting intelligence community document exploitation objectives from criminal law enforcement forensics and counterintelligence perspectives. DC3 provides computer investigation training to forensic examiners, investigators, system administrators, and any other DOD members who must ensure Defense information systems are secure from unauthorized use, criminal and fraudulent activities, and foreign intelligence service exploitation. DC3 remains on the leading edge of computer technologies and techniques through research, development, testing, and evaluation applied to digital evidence processing and computer forensic analysis; and by partnering with governmental, academic, and private industry computer security officials.

1.2 Overview

The DC3 Challenge encourages innovation from a broad range of individuals, teams, and institutions to provide technical solutions for computer forensic examiners in the lab as well as in the field. Approximately 22 different challenges ranging from basic forensics to advanced tool development are being provided to all participants. The challenges are single based challenges and are designed to be unique and separate from one another. This format is different than the whole forensic process scenario, with incorporated challenges, provided for the 2009 DC3 Challenge.

1.3 Objectives

The objectives of the Annual Digital Forensics Challenge are to establish relationships; resolve technological issues; and develop new tools, techniques, and methodologies for the digital forensic community.

2.0 ELIGIBILITY CRITERIA

2.1 Registration

Registration is designed to be completed online via the DC3 2010 Challenge website at http://www.dc3.mil/challenge/2010. Registration must be for all team participants in its entirety. If there is any 'anonymous' information supplied with application submittal, the application will be denied. In the unlikely event that the website is not functioning, a team member can provide the necessary information in an email to challenge@dc3.mil or call the DC3 challenge line at 410-981-6610.

2.2 Requirements

Challenge entry is open to both individuals and teams. Teams may include corporate or academic entities but are not limited to these. Each entry must meet the following eligibility requirements:

1. An individual cannot participate on more than one (1) team or compete with multiple entries.

2. Teams will consist of one (1) to four (4) member(s).

3. The team's first team member will be assigned as the team leader and considered the sole Point of Contact (POC).

4. All members are required to provide their personal information (Full Name, Address, Telephone Number, Email Address, Etc) for team approval.

    a. *Failure to provide accurate personal information OR falsifying registration information will deny your application and/or disqualify your team from challenge participation* as per Section 8.0 – Team Disqualification.

    b. All changes to team members (add/update/remove) and their related information are the responsibility of team POC to update with the DC Challenge Team in writing to challenge@dc3.mil

5. Team and Team Member Affiliations

    a. Team member affiliations are required at time of registration by the DC3 Challenge for determining team affiliation at team approval.

    b. Each team member's affiliation should be relevant to when team challenge packet is submitted (NOT when registered):
        i. ***Civilian*** – A person or team **NOT** attending a High School, College/University/Technical school facility, in the Military, working for the Federal Government or working in the Commercial / Private Sector.
        ii. ***Commercial*** – A person or team that is employed for a Commercial/Private Sector company. This includes contractors that work for Military, Federal, State and Local Government agencies.
        iii. ***Government*** – A person or team that works for their nation's Federal, State, or Local Government agency. This excludes contractors.
        iv. ***Military*** – A person or team that is employed by their nation's Military.
        v. ***High School Student*** – A person or team that is attending a high school and has **NOT** graduated before the submission of the final Challenge package.
        vi. ***High School Faculty*** – A person or team that teaches students in a High School facility. Faculty that does not teach is considered Civilian.
        vii. ***Undergraduate Student*** – A person or team that is attending a College/University/Technical School and has **NOT** graduated before the submission of the final Challenge package.
        viii. ***Undergraduate Faculty*** – A person or team that teaches at a College/University/Technical School facility.

ix. ***Graduate Student*** – A person or team that is attending a graduate school and has **NOT** graduated before the submission of the final Challenge package.
x. ***Graduate Faculty*** – A person or team that teaches at a Post Graduate facility.

c. The overall team affiliation is calculated by the DC3 Challenge team based on the provided team member(s) affiliation(s).
   i. If a team consists of all the same team member affiliation (i.e. 4 Government members), the team will be assessed by its common member affiliation (i.e. Government.)
   ii. If a team consists of all academic students or of all academic faculty members, the highest category level will be assessed as the team affiliation. See Section 5.3 – Academic criteria for additional details.
   iii. If a team consists of a mix of 2 or more team member affiliations that are not all academic (i.e. 2 Civilian and 1 High School Student), the team will be assessed as the lowest team affiliation of Civilian.

d. Once team affiliation is determined by the DC3 Challenge team, the available prizes are assigned based on the team's eligibility to the prize(s). See Section 5.2 - Prize Eligibility for further details.

e. Any changes of team member affiliation after approval to participate should be submitted to the DC3 Challenge team at challenge@dc3.mil by the POC at time of change. Failure to report team member affiliation changes will be cause for disqualification as per Section 8.0 – Team Disqualification.

6. All team members must of the same citizenship category (U.S. or Non-U.S.) to compete for prize winnings. If any member on the team is not of the same U.S. or Non-U.S. citizenship as the other team members, graded for "Points-only" and no Prizes will be awarded.

7. If participant is under the age of 18, the team member(s) is required to provide written authorization from a parent / legal guardian via the DC3 Permission to Participate form. Failure to provide this written permission will be cause for disqualification as per Section 10.0 – Team Disqualification.

8. DC3 employees, current and former within the past year (2009), and their relatives are ineligible to participate for prizes, however can compete for points.

3.0 SPONSORSHIP

The SysAdmin, Audit, Network, Security (SANS) Institute the largest source for information security training, certification, and resource in the world, and IMPACT, the first global public-private initiative against cyber-terrorism are co-sponsoring the 2010 DC3 Challenge.

3.1 SANS Institute

The SysAdmin, Audit, Network, Security (SANS) Institute is the most trusted and by far the largest source for information security training and certification in the world. It also develops, maintains, and makes available at no cost, the largest collection of research documents about various aspects of information security, and it operates the Internet's early warning system - Internet Storm Center. SANS is also a sponsor in the U.S. Cyber Challenge, ran by the Center for Strategic & International Studies (CSIS).

3.2 IMPACT

The International Multilateral Partnership Against Cyber-Threats (IMPACT) is the first global public-private initiative against cyber-terrorism. IMPACT is dedicated to bringing together governments, industry leaders and cyber security experts to enhance the global community's capacity to prevent defend and respond to cyber threats. IMPACT and DC3 have partnered to provide a Digital Forensic Challenge opportunity for non-U.S. entries. This opportunity will provide an international aspect to a previously U.S.-based event and allow additional insight into global methods to fight cyber crime.

4.0 THE CHALLENGE

4.1 Challenge Objectives

The Objectives of the Annual Digital Forensics Challenge are to:

- Establish relationships within the Digital Forensics Community;
- Resolve issues facing the Digital Forensics Community;
- Develop new tools, techniques, and methodologies for the Digital Forensic Community

4.2 Challenge Rules

The Challenge Rules are published on the DC3 Challenge Website (www.dc3.mil/challenge) and are subject to change. All changes will be documented as they occur. Please review and refer back on a regular basis to ensure that compliance in all areas is maintained.

4.3 Challenge Grading

There are 22 single scenario based problem challenges. The chart of each specific challenge and corresponding points can be found in the Appendix under A-2 Challenges and Point Structure. There are four (4) 100 point challenges, five (5) 200 point challenges, four (4) 300 point challenges, three (3) 400 point challenges, and six (6) 500 point challenges.

4.4 Challenge Schedule / Key Dates

- **4 Dec 2009 – Announcement of DC3 Challenge 2010**
- **15 Dec 2009 - Registration Begins**
  - Registration and Challenge packets containing all of the challenge materials will be available for download only on or about 15 December 2009.
  - Applications received each day by close of business (COB) will be available
- **26 Jan 2010 – Press Release** and official announcement at the 2010 DC3 Cyber Crime Conference, St. Louis, MO
- **2 Nov 2010 – Submission Entry Deadline**
  - All Challenge solution packages, including scripts and non-commercial programs created by the team, must be uploaded to DC3 no later than 11:59 PM EST to be eligible for a prize in their assigned category.
  - Challenges solution packages mailed via US Postal Service, Federal Express, or anything other than electronic submittals MUST be postmarked by 11:59 PM EST on 1 Nov 2010 to be eligible for a prize in their assigned category.
  - Challenge solutions received after 1 November 2010 EST will not be accepted for prizes. Scoring after this date will be per the DC3 Challenge Team's discretion.
- **1 Dec 2010 – DC3 Challenge Winners Announced**
  - All participants will be notified via email of the posting of Challenge scoring results to the DC3 Challenge Website.
  - Final results will be posted on the DC3 Challenge Website.
  - In the event of a tie score for the top challenge solution package, the tie will be broken by the time difference between INITIAL download of challenge packet and submittal (by electronic upload or postmarked date) of the team's solution packets.

5.0 PRIZE CRITERIA

5.1 Prizes

Based upon their team affiliation criteria, several prizes are available to Challenge teams based on their team's eligibility per prize provided by the DC3 Challenge sponsor's requirements.

Each member of the winning team will also receive a plaque as well as formal recognition at the conference by DC3.

5.2 Prize Eligibility

5.2.1 DC3 Prize Requirements

The winning teams of the Civilian, Corporate / Private Sector, Federal Government, Military, High School Faculty, Undergraduate Faculty, or the Graduate categories will receive a trip to the 2011 DoD Cyber Crime Conference by DC3, based on government per Diem (airfare, lodging, meals, and paid conference fees) for up to 4 members.

Additional prize eligibility requirements are as follows:

- All team members must hold U.S. citizenship.
- All team members must be able to travel from within the Continental United States in order to claim the trip to the Conference (U.S. citizens abroad are eligible providing they transport themselves to the Continental United States.)
- All team members must meet all other previously stated Challenge Rules and Requirements.
- Any team or team member(s) under the age of 18 must provide written permission to participate in the challenge.

5.2.2 SANS Prize Requirements

The winning teams of the High School, Undergraduate, and Graduate student academic categories will receive a trip to the 2011 DoD Cyber Crime Conference by SANS.

- All team members must hold U.S. citizenship.
- All team members are actively attending as a U.S. student at a U.S. High School, U.S. Undergraduate or U.S. Graduate College upon submission of your results as per the Academic Criteria in Section 5.3.
- Be able to travel from within the Continental United States in order to claim the trip to the Conference (U.S. citizens abroad are eligible providing they transport themselves to the Continental United States).
- All team members must meet all other previously stated requirements of the Challenge Rules.

5.2.3 IMPACT Prize Requirements

The winner(s) of the International category from an IMPACT-member country will be eligible to fly to Malaysia for a tour of the IMPACT facility in Cyberjaya. They will be officially presented with a commemorative plaque and potential grants of EC-Council and SANS courses. The results of the IMPACT/DC3 Challenge winner will be presented at the Department of Defense Cyber Conference in January 2011, and published for community utilization.

In addition to the DC3 team requirements, the below are additional IMPACT requirements:

- All team participants DO NOT hold U.S. citizenship.
- All team members' legal residences are located outside of the U.S. *AND* in an IMPACT member country (any country listed on the following website http://www.itu.int/cgi-bin/htsh/mm/scripts/mm.list?_search=ITUstates
- All team members must meet all other non-U.S. Challenge Rules and Requirements.
- All current DC3 or IMPACT personnel and former DC3 or IMPACT personnel who are within one calendar year (1 Jan 2009) are ineligible to participate.

For more information on IMPACT participation requirements, visit the IMPACT website at www.impact-alliance.org under events / upcoming / IMPACT/DC3 Challenge.

5.3 Academic Criteria

Should an academic category be selected as a team category, the following applies:

- Team member must be enrolled and in good standing for the academic institution attending ON the date you submit your solutions package to be eligible for placement in the Academic category.
  - Proof of enrollment must be provided
  - A letter or fax on the institution letterhead, signed by team member and institution administrative office will suffice
  - Age of the player on the date of the Challenge solution is submitted does not matter
  - Failure to provide proof of enrollment with appropriate signatures will disqualify the team from the Academic category and will be placed in the Civilian / Private Sector category.
- If the team consists of students from different academic categories (e.g. 2 high school students, 1 undergraduate student, and 1 graduate student), the highest category level will be used to assess the category status for the team. In the example above, the team's category would be designated as Graduate students.

5.3.1 Graduate

- Individuals / Team status **will be** placed in the **Graduate (PG)** category if they are still in a Graduate school on the date when the Challenge 2010 package **is submitted** (*not when you apply*).
- PG team (s) who submits their package **prior** to graduating will be placed in the PG category.
- PG team (s) who submits their package **after** graduating will be placed in the category of Military, Federal Government, or Commercial/Private Sector and are ineligible for Academic recognition.
- Should the Individual / Team member have a change in their expected graduation date, they **must** inform the DC3 Challenge staff (i.e. anticipated Graduation Aug 2010 changes to Dec 2010 – status will remain in the PG category). Proof of this change will have to be provided.

5.3.2 Undergraduate

- Individuals /Team status **will be** placed in the **Undergraduate (UG)** category if they are still in an Undergraduate program on the date when the Challenge 2010 package **is submitted** (*not when you apply*).
- UG team (s) who submits their package **prior** to graduating will be placed in the UG category.
- UG team (s) who submits their package **after** graduating but while attending a graduate program will be placed in the PG category.
- UG person(s) who submits their package **after** graduating but **not** attending a graduate program will be placed in the category of Military, Federal Government, Commercial/Private, or Civilian and will be ineligible for Academic recognition.

5.3.3 High School

- Individuals / Teams **will be** placed in the **High School (HS)** category on the date when the Challenge 2010 package **is submitted** (*not when you apply*).
- HS senior(s) or Team with a HS senior member who submits their package **prior** to graduating will be placed in the HS category.

- HS senior(s) or Team with a HS senior member who submits their package **after** graduating, but while attending college/university/technical program will be placed in the Undergraduate (UG) category.
- HS senior(s) or Team with a HS senior member who submits their package **after** graduating, but **not** attending college/university/technical program will be placed in the category of Military, Federal Government, Commercial/Private, or Civilian and will be ineligible for Academic recognition.

5.4 Judging and Challenge Rules

Challenge Judges will adjudicate and resolve any discrepancies throughout the grading process. In the event of a tie for equal points, the team providing the challenge submissions with the shortest amount of time (based on the difference of the time between the INITIAL challenge approval email and the team submission to the DC3) will be declared as the winner. All decisions of the DC3 Challenge judging are final.

By submitting a proposed solution to the DC3 Challenge, you agree to the following terms:

- Solutions and answers have been checked for viruses, trojans, and malicious code using commercially available antivirus software and certify that it is free of those malicious computer programs.
- If in the winning category, **ALL** team members must agree to have their name(s) and other personal information used in promoting the DoD Cyber Crime Conference.
- DC3 is the final arbiter of any dispute concerning interpretation of the rules for the DC3 Challenge. **ALL DECISIONS ARE FINAL.**

6.0 INTELLECTUAL PROPERTY

All tools and methods created by the Challenge participants will remain the intellectual property of the creator(s). DC3 reserves the right to request to copy of all tools, scripts, and methods/techniques for our independent testing and validation. Failure to provide the required tools, scripts, and methods / techniques upon request will disqualify the team from the DC3 Challenge participation.

All submissions with team-created tools, techniques, solutions, and responses, in their entirety, may be shared, in their entirety, with the Challenge participants, DOD partners, and the digital forensics community by Challenge Team Names Only. These tools, techniques, solutions, and responses may be documented and publicized.

To evaluate efficiency, DC3 will require the following upon Challenge submission:

- For each tool, script, and method / technique, documentation and a description of the steps used to accomplish the Challenge solution(s).
- A copy of each non-commercial tool and/or script OR modified open-source tools and/or scripts used to accomplish the Challenge solution(s).
- If the tool, script, and method / technique or modification is an open source product, a URL to the site from the open source sharing site must be provided. Examples of the open source sharing sites include Source Forge, Google Code, Code Plex, etc.

7.0 LIMITATION OF LIABILITY

The computer data and media supplied for the DC3 Challenge has been checked for computer viruses, Trojans, and other malicious code using commercial antivirus software configured with current signatures as of Dec 2009 and is found to be free of such programs. If the materials received appear tampered with discontinue use immediately and return the materials to DC3.

In consideration of participating in the DC3 challenge, contestants acknowledge that DC3 is not responsible for any damage caused to any computer or network due to the loading of, or operation of the storage media holding the DC3 Challenge materials.

8.0 TEAM DISQUALIFICATION

Registered individuals/teams will be disqualified for any of the following reasons:

- Failure to provide accurate personal information and/or falsifying registration information
- Failure to provide scripts, programs, and/or methods referenced in Section 6.0 Intellectual Property in the DC3 Challenge Rules
- If at the time of submission grading and verification, it is determined that a team or member of a team has not met the eligibility requirements, the entire team shall be terminated without regard to Challenge performance in meeting prize objectives
- Failure to submit documents by the required solution due date
- Fraudulent acts, statements, or misrepresentations involving any DC3 or other federal government documentation or systems used for the challenge.
- Violation of any federal, state, or local law or regulation determined to be inconsistent with the DC3 Challenge.
- Any team member under the age of 18 must submit a DC3 Permission to Participate form, signed by a parent / legal guardian to participate in the Challenge. If, it is discovered that a team member is under the age of 18 and has not submitted this form, the team will be immediately disqualified.

9.0 CHALLENGE CANCELLATION

The DC3 reserves the right to cancel this challenge at any time leading up and during the Challenge time frame.

10.0 PRIVACY POLICY

All Team information, except Team Name, will remain anonymous from being able to identify a team or its members throughout the Challenge process, unless prior written approval by the Challenge team members to release that information is provided OR the team has been declared a winner of the Challenge.

DC3 Challenge will remain the primary contact for any request for contact information for Challenge teams during the Challenge process. These requests will be routed by DC3 Challenge to the Challenge team leader for approval for release. It is the Challenge team's discretion to be contacted by the interested party outside of DC3 thereafter.

For DC3 Challenge and U.S. Cyber Challenge promotional purposes, specific anonymous information may be shared with 3rd parties. This information will be unassociated from Team Names and their Team Member's personal and contact information unless prior written approval for release said information has been provided by the Team and its Members directly to DC3 Challenge. This information includes the following:

- Member affiliations, states, and countries from Team Members as part of the statistical reporting of the DC3 Challenge's progress with the public and press.
- Member affiliations, U.S. citizenship, schools, states, zip codes, and countries from Team Members with the DC3 Challenge sponsors/partners and DOD partners as part of government/academic Cyber Challenges.

APPENDIX

A-1: Challenges and Point Structure

Points	Challenge Title
100	Missing File Header Reconstruction
100	Detect Suspicious Software
100	Registry Analysis
100	Metadata
200	Audio Steg
200	Keylog Cracking
200	Password Cracking
200	Steg S-Tools
200	NTFS File Record challenge
300	PCAP Data Recovery
300	Compromised Host Disk Image Analysis
300	PAX Cracking
300	Accessing the Shadow Volume on Password Protected Vista Platform
400	Windows 7 USB Thumb Drive Encryption
400	Extracting Hidden Evidence in a VMware / WinXP Virtual Machine
400	Steganography
500	MFT File Reader Tool Development
500	Text String Search Tool Development
500	Language Identifier Tool Development
500	Data Recovery from HPA as a Universal Tool or per Manfacturer Tool Development
500	Data Recovery from a Unmarried TPM System Hard Drive Tool Development
500	Automatically Parse Shadow Copy Files Tool Development